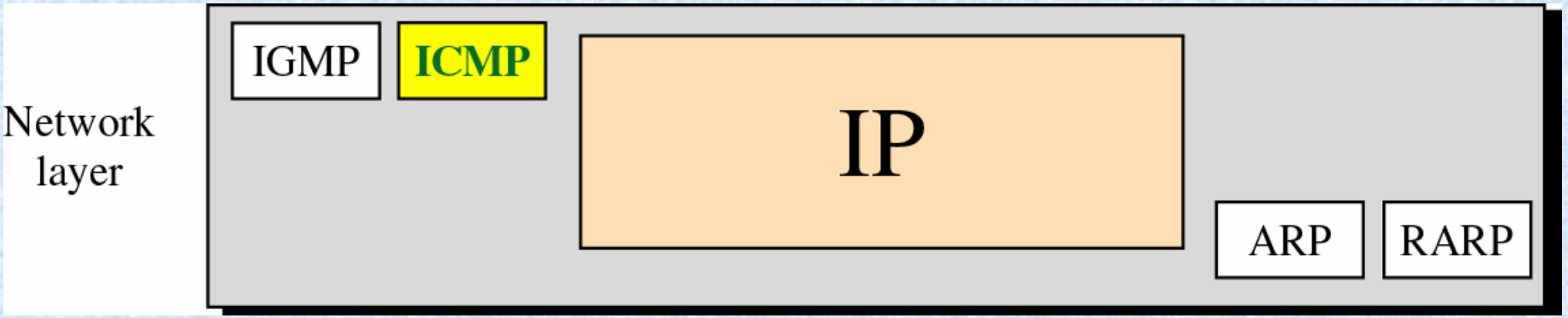
Chapter 9

Internet Control Message Protocol (ICMP)

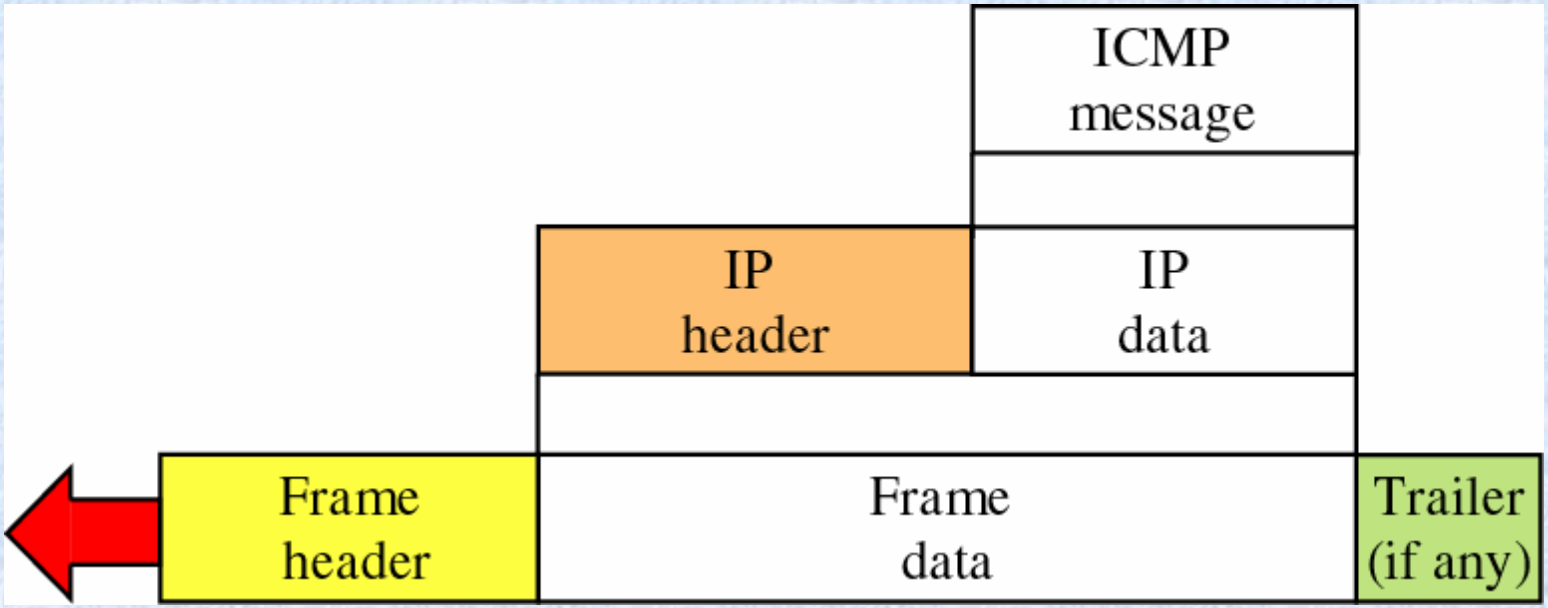
CONTENTS

- TYPES OF MESSAGES
- MESSAGE FORMAT
- ERROR REPORTING
- QUERY
- CHECKSUM
- ICMP PACKAGE

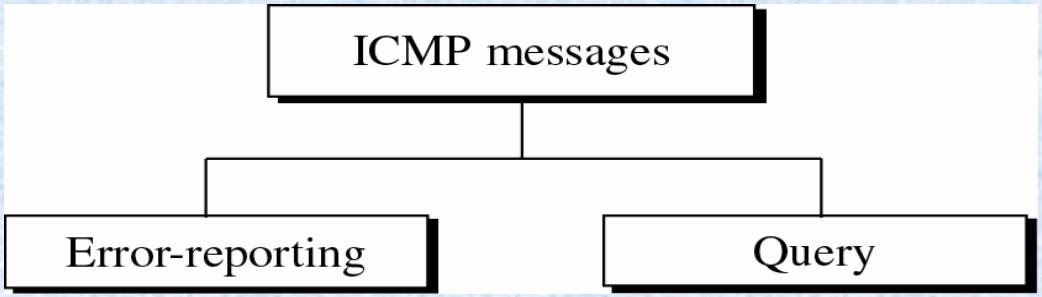
Position of ICMP in the network layer



Encapsulation of ICMP packet

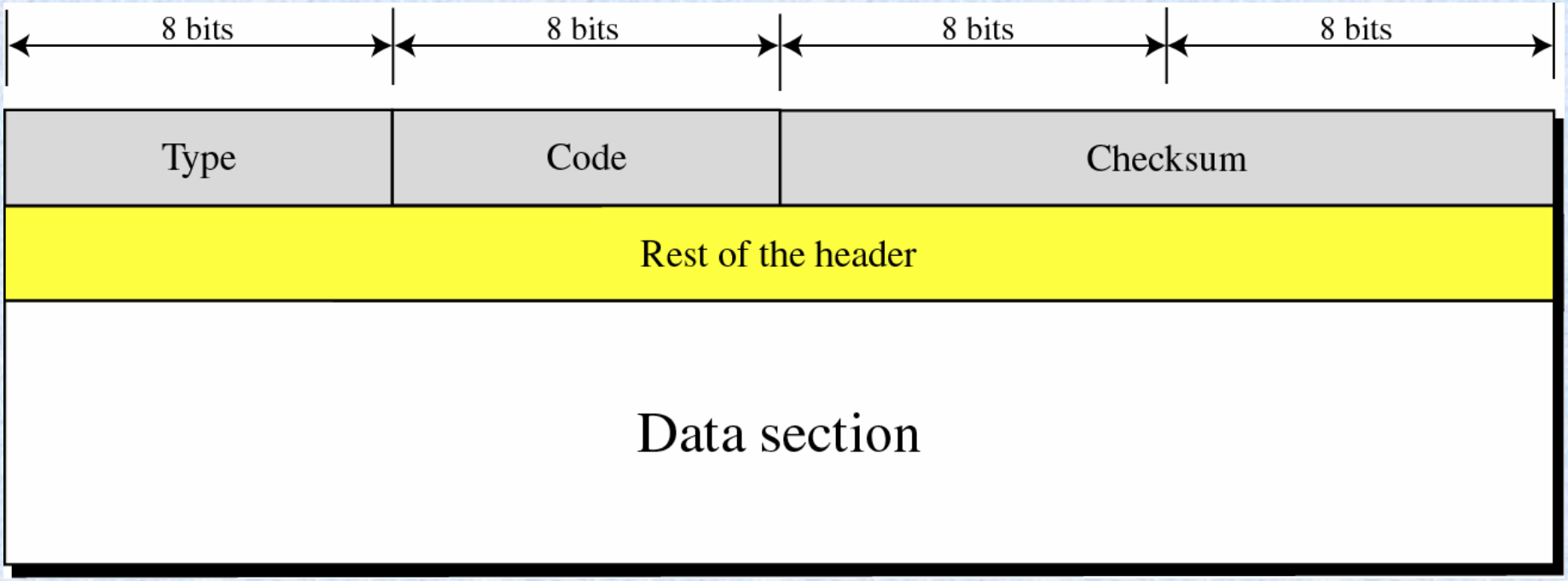


9.1 TYPES OF MESSAGES



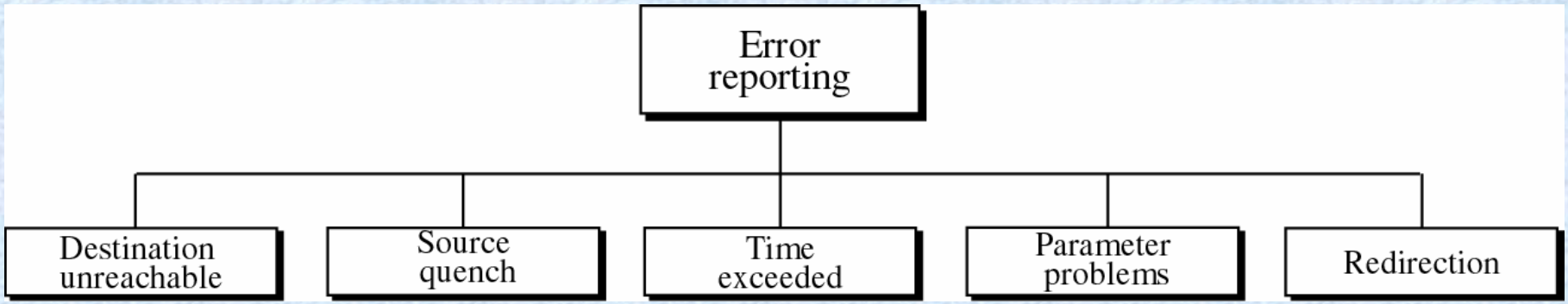
Category	*Type*	*Message*
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router solicitation or advertisement

9.2 MESSAGE FORMAT



9.3 ERROR REPORTING

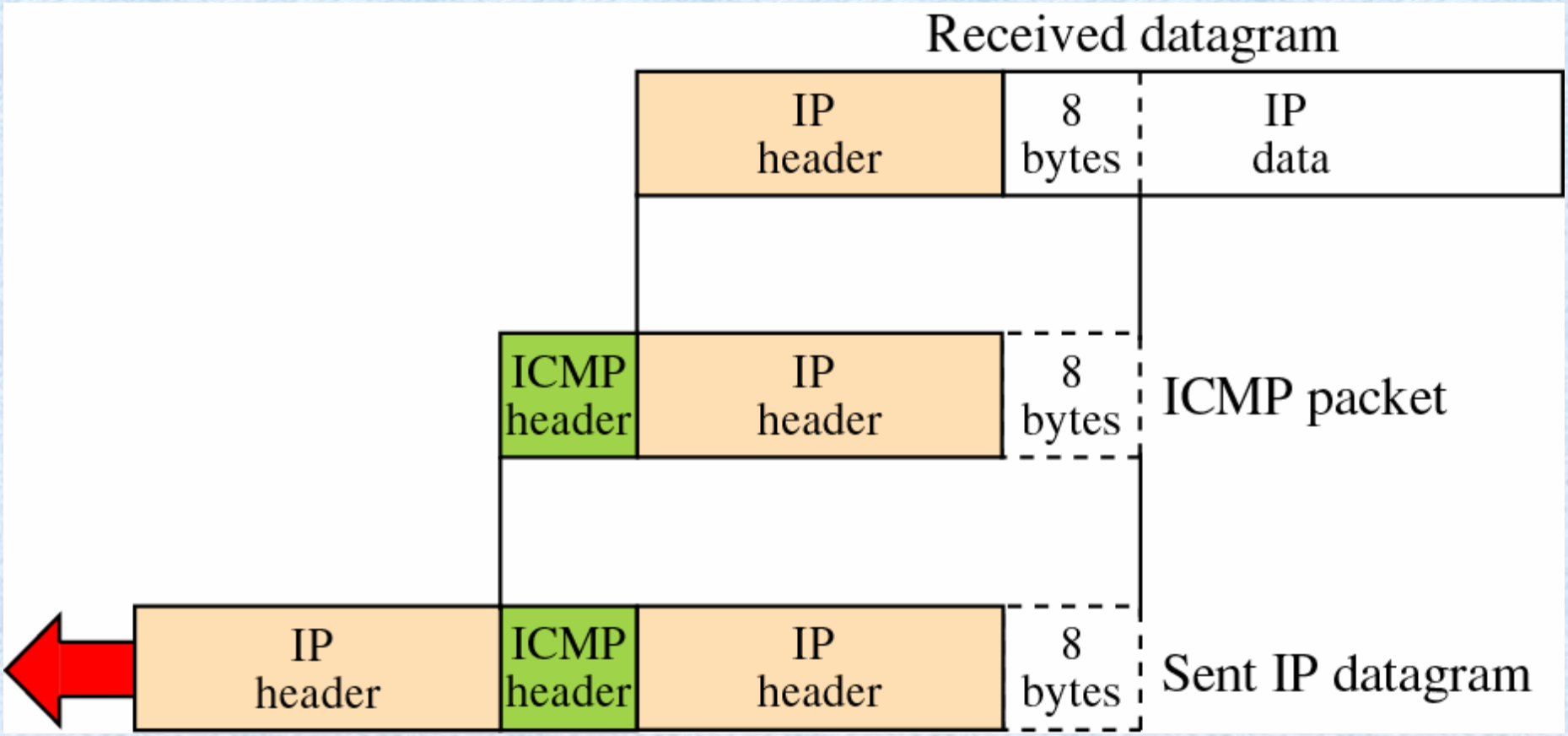
ICMP always reports error messages to the original source.



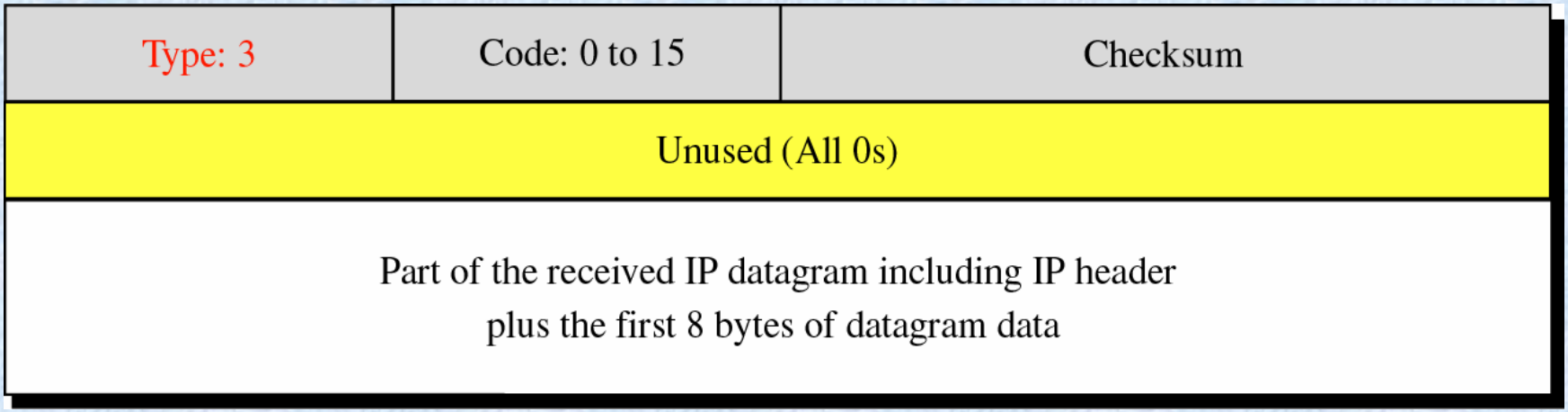
Important points about ICMP error messages:

1. ***No ICMP error message for a datagram carrying an ICMP error message.***
2. ***No ICMP error message for a fragmented datagram that is not the first fragment.***
3. ***No ICMP error message for a datagram having a multicast address.***
4. ***No ICMP error message for a datagram with a special address such as 127.0.0.0 or 0.0.0.0.***

Contents of data field for error messages



Destination-unreachable format

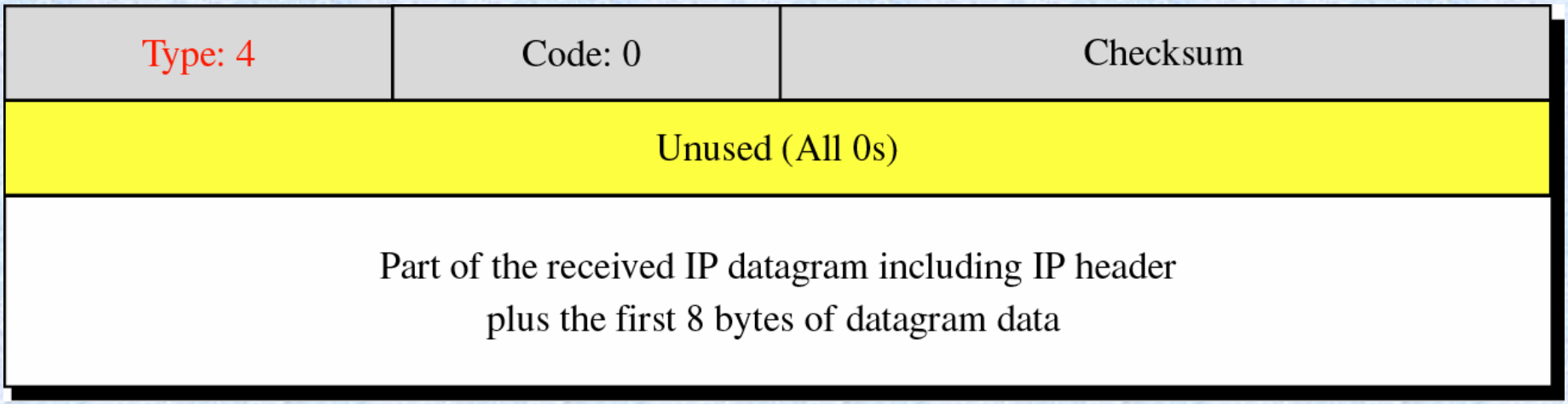


Code	Error	Code	Error
0	Network unreachable	8	Isolated Source Host
1	Host unreachable	9	Comm. with destination network prohibited
2	Protocol unreachable	10	Comm. with destination host prohibited
3	Port unreachable	11	Network unreachable – Type of Service
4	Fragmentation required, but prohibited	12	Host unreachable – Type of Service
5	Source routing is infeasible	13	Host unreachable – Administrative Filter
6	Unknown destination network	14	Host unreachable – Precedence violated
7	Unknown destination host	15	Host unreachable – Precedence cut off

- ***Destination-unreachable messages with codes 2 or 3 can be created only by the destination host. Other destination-unreachable messages can be created only by routers.***
- ***A router cannot detect all problems that prevent the delivery of a packet.***

Source-quench

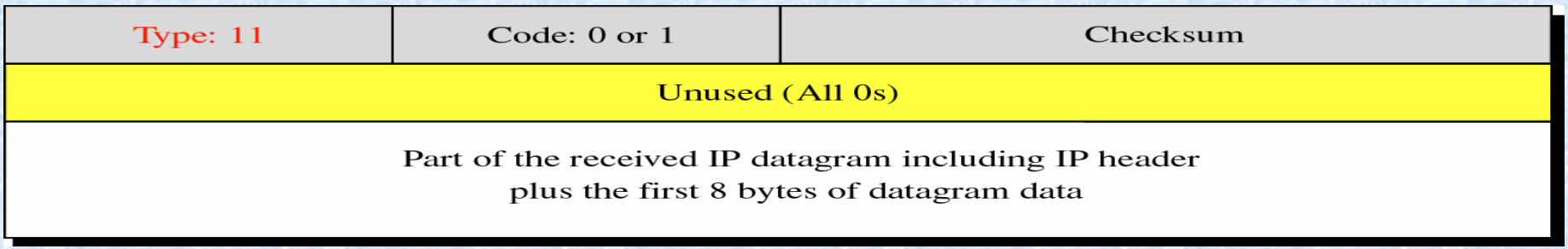
- ***There is no flow-control mechanism in the IP protocol.***



- ***A source-quench message informs the source that a datagram has been discarded due to congestion in a router or the destination host.***
- ***The source must slow down the sending of datagrams until the congestion is relieved.***
- ***One source-quench message should be sent for each datagram that is discarded due to congestion.***

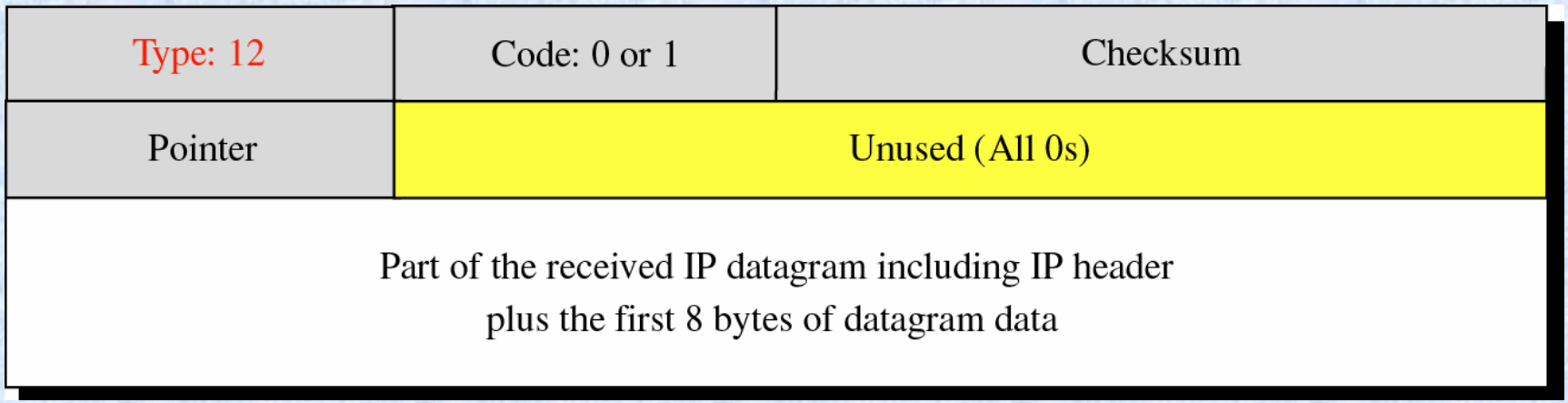
Time Exceeded

- ***Whenever a router receives a datagram with a time-to-live value of zero, it discards the datagram and sends a time exceeded message to the original source.***
- ***When the final destination does not receive all of the fragments in a set time, it discards the received fragments and sends a time-exceeded message to the original source.***
- ***In a time-exceeded message, code 0 is used only by routers to show that the value of the time-to-live field is zero. Code 1 is used only by the destination host to show that not all of the fragments have arrived within a set time.***



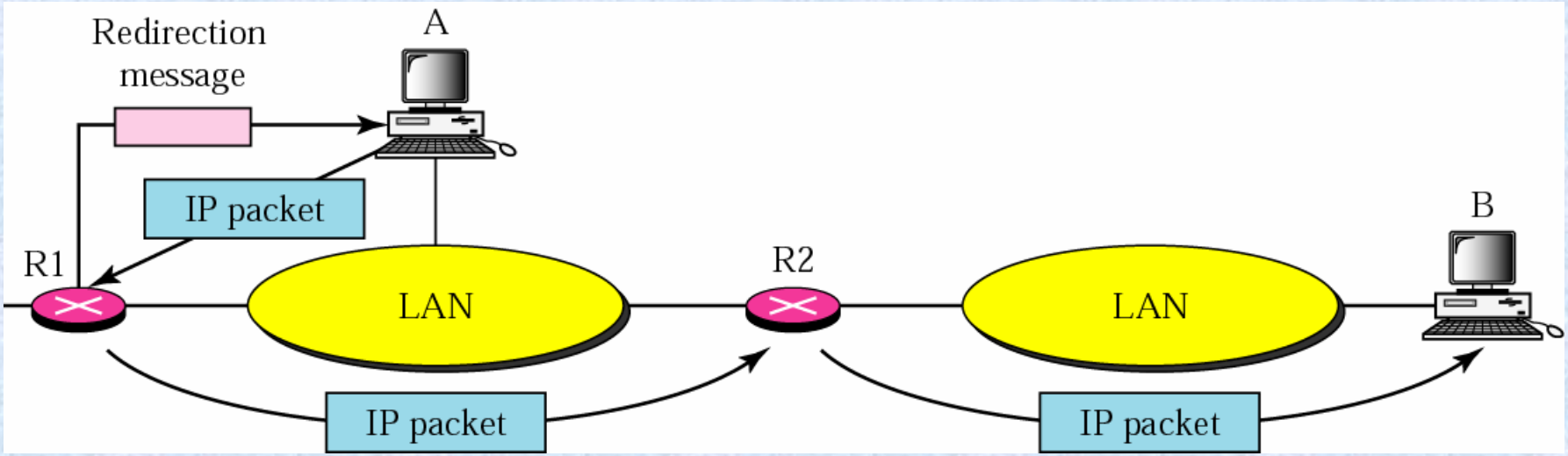
Parameter Problem

A parameter-problem message can be created by a router or the destination host.



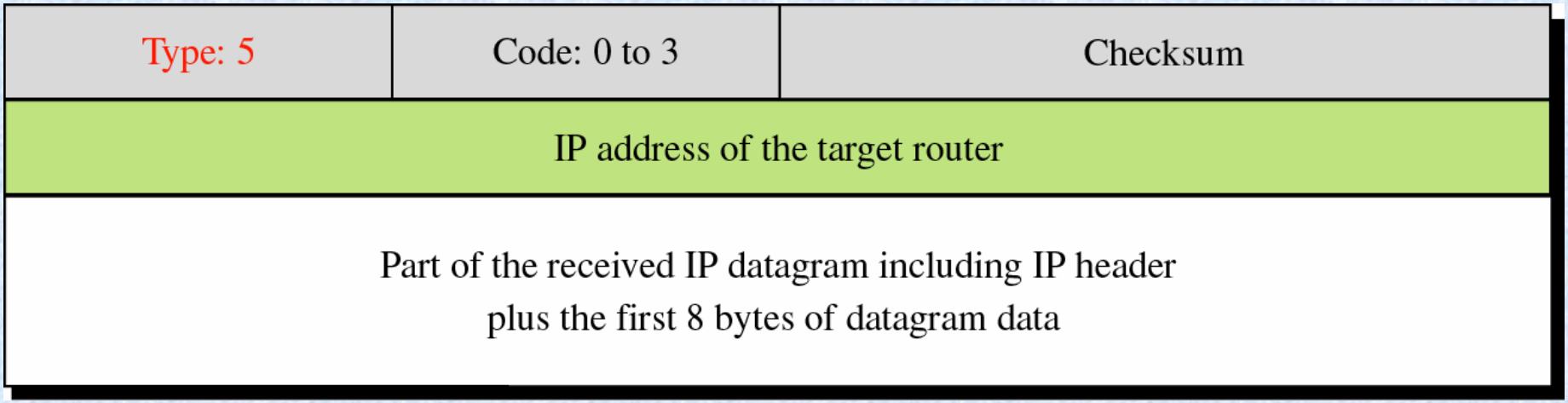
C

Redirection concept



A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message.

Redirection message format

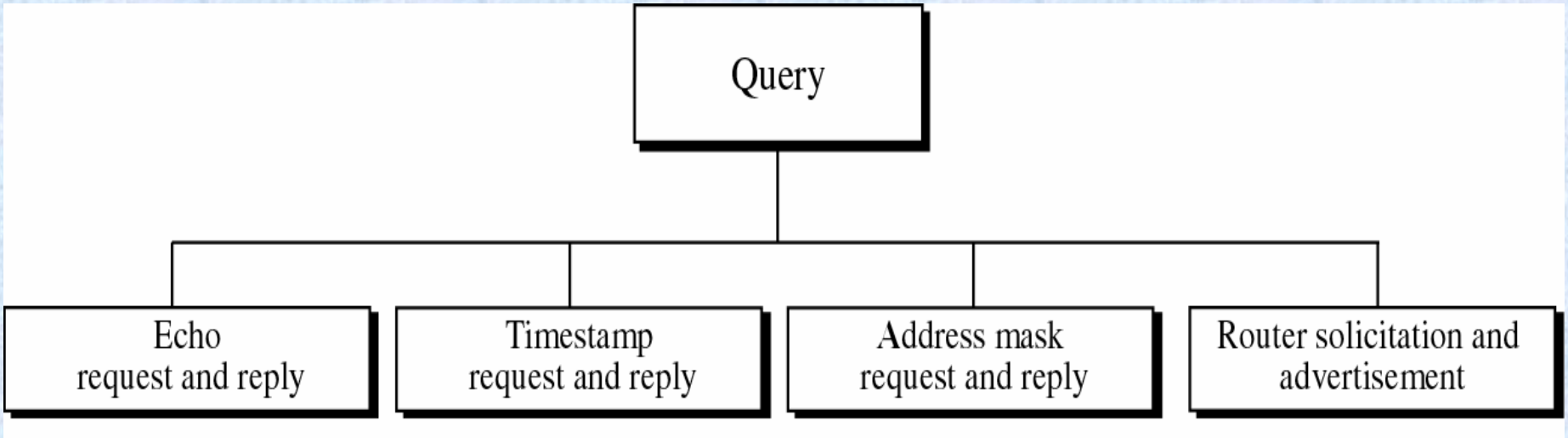


Code 0: Network specific
Code 1: Host specific

Code 2: Network specific (specified service)
Code 3: Host specific (specified service)

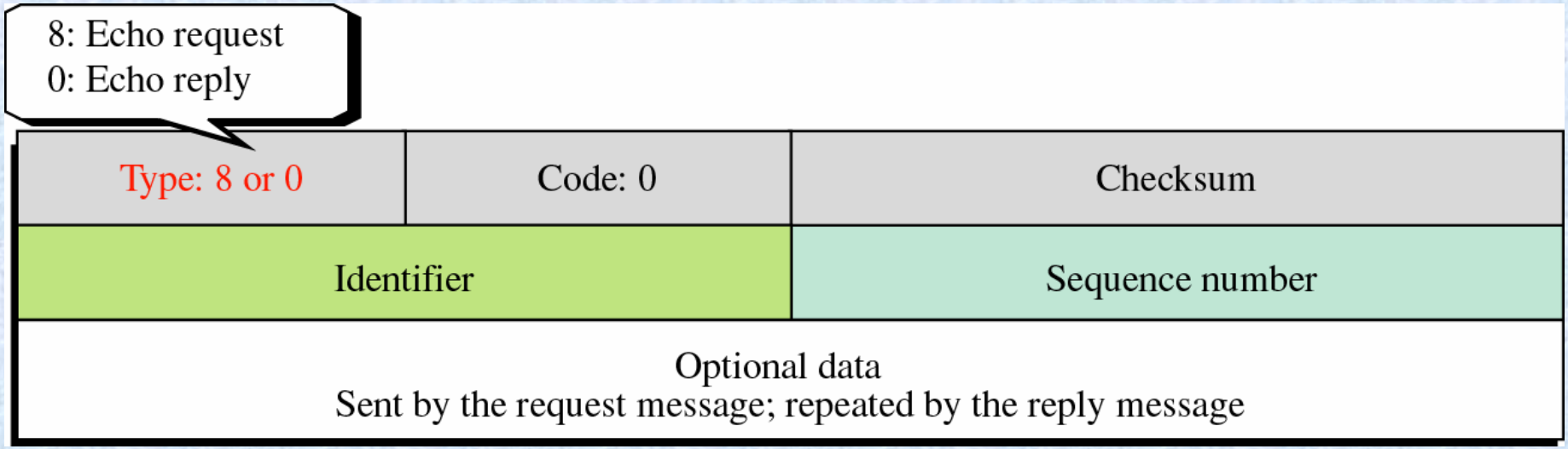
A redirection message is sent from a router to a host on the same local network.

9.4 QUERY

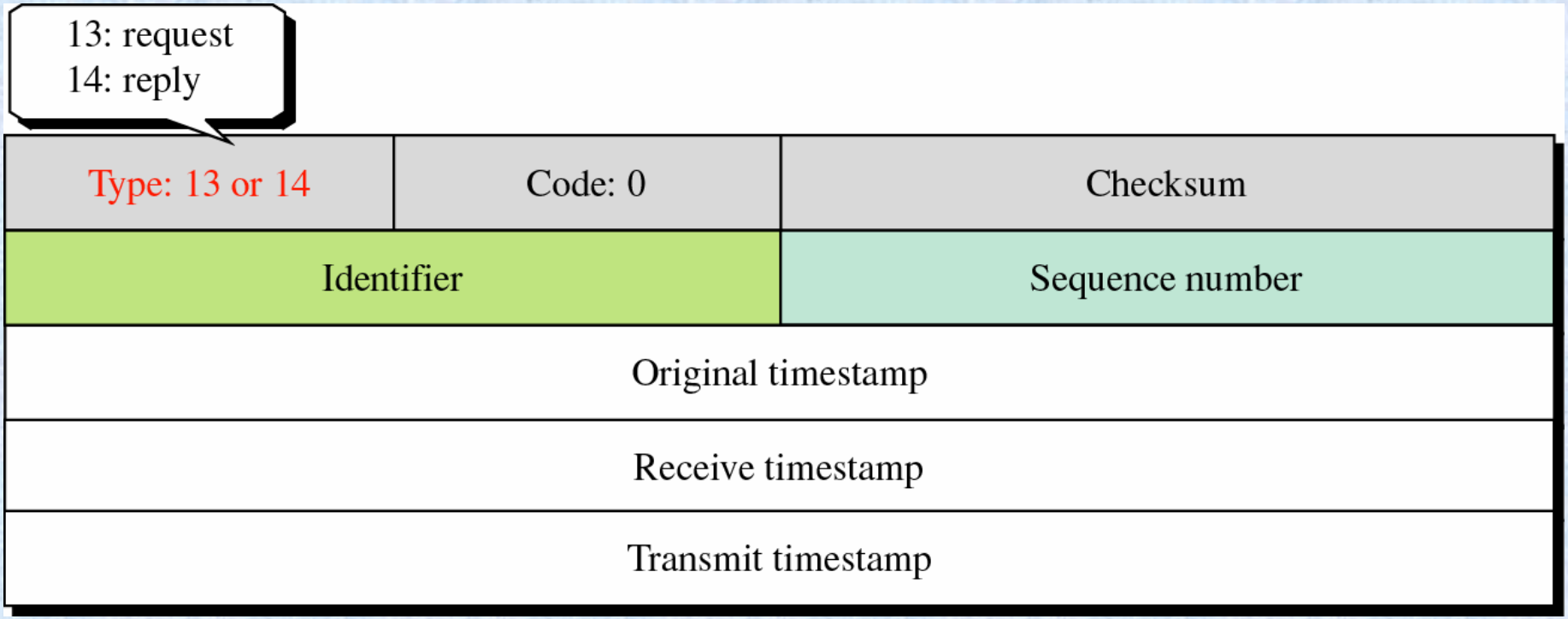


Echo Request & Reply

- An echo-request message can be sent by a host or router.
- An echo-reply message is sent by the host or router which receives an echo-request message.
- Echo-request and echo-reply messages can be used by network managers to check the operation of the IP protocol
- Echo-request and echo-reply messages can test the reachability of a host. This is usually done by invoking the ping command.



Timestamp-request and timestamp-reply message



Sending time = value of receive timestamp – value of original timestamp

Receiving time = time the packet returned – value of transmit timestamp

Round-trip time = sending time + receiving time

Timestamp-request and timestamp-reply messages can be used to calculate the round-trip time between a source and a destination machine even if their clocks are not synchronized.

Given the following information:

Value of original timestamp: 46

Value of receive timestamp: 59

Value of transmit timestamp: 60

Time the packet arrived: 67

We can calculate:

Sending time = 59 – 46 = 13 milliseconds

Receiving time = 67 – 60 = 7 milliseconds

Round-trip time = 13 + 7 = 20 milliseconds

The timestamp-request and timestamp-reply messages can be used to synchronize two clocks in two machines if the exact one-way time duration is known.

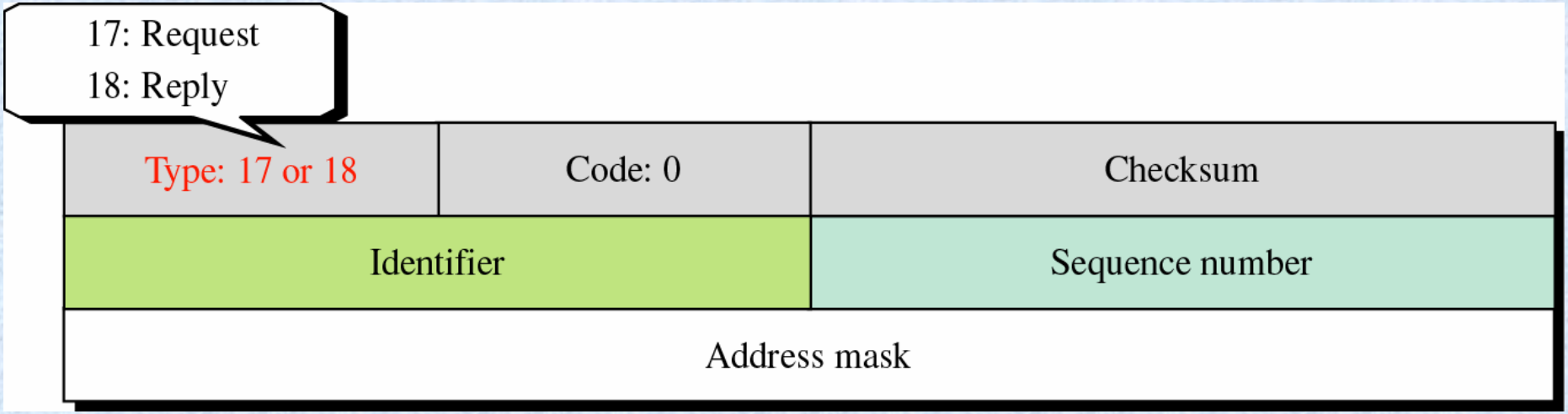
Given the actual one-way time,

Time difference = receive timestamp – (original timestamp field + one-way time duration)

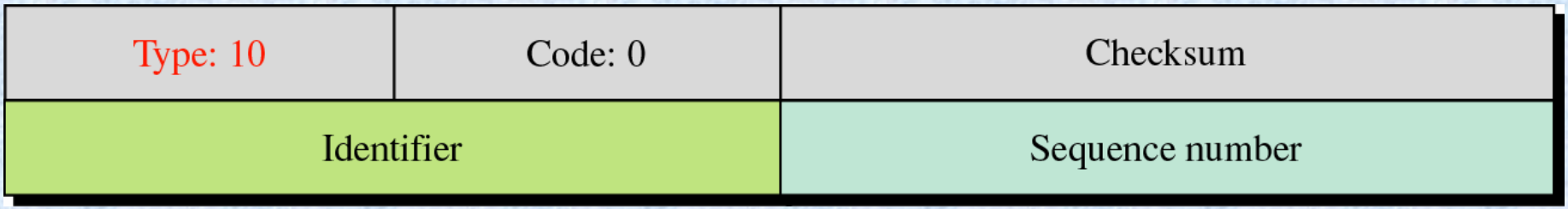
We have:

Time difference = 59 – (46 + 10) = 3

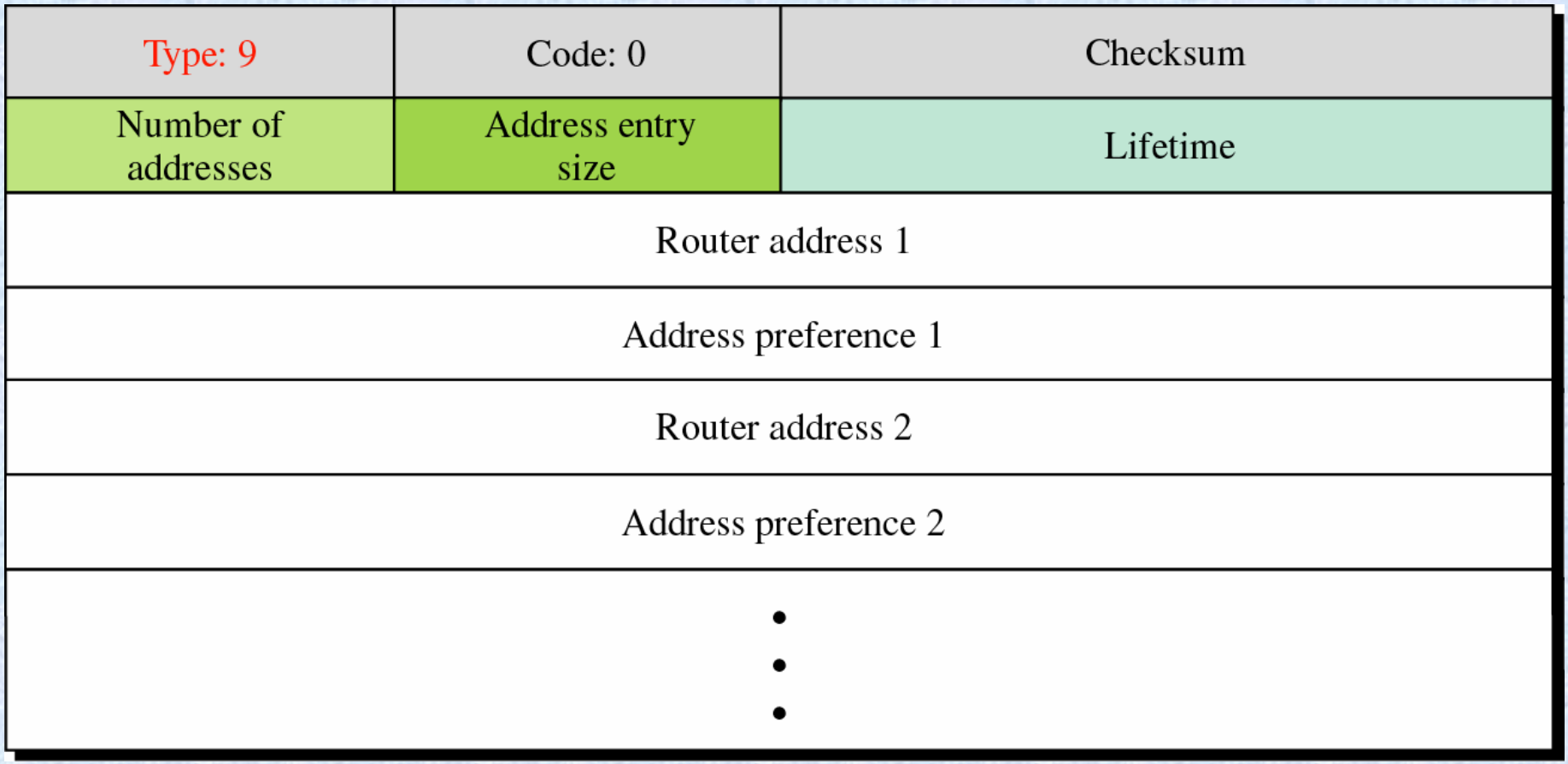
Mask-request and mask-reply message format



Router solicitation message format



Router advertisement message format



9.5 CHECKSUM

8	0	0
1		9
TEST		

8 and 0	→	00001000 00000000
0	→	00000000 00000000
1	→	00000000 00000001
9	→	00000000 00001001
T & E	→	01010100 01000101
S & T	→	01010011 01010100
Sum	→	10101111 10100011
Checksum	→	01010000 01011100

9.6 ICMP PACKAGE